Διασύνδεση με social media

|  |
| --- |
| **Σημαντική εξέλιξη**: Το Twitter api δεν υποστηρίζει τη δυνατότητα να σου επιστρέψει το verified email του χρήστη. Επίσημα υποστηρίζουν ότι αν χρειάζεσαι το email κάποιου χρήστη, τότε να το ζητήσετε στο δικό σας site. Αυτό πρακτικά δυσκολεύει την διαδικασία του login using twitter γιατί υποθέταμε ότι θα κάναμε match το email που μας δίνουν τα social media με το email κάποιου υπάρχοντος χρήστη.  ([https://dev.twitter.com/docs/faq#6718](https://dev.twitter.com/docs/faq%236718)) |

# Διαδικασία σύνδεσης

1. Ο χρήστης πατάει το κουμπί για να συνδεθεί μέσω ενός social media και εφόσον υπάρχει κάποιο active3 account με το ίδιο email θα προχωρώ σε αυτόματη σύνδεση του χρήστη και στο active3 και τον κάνω redirect στην σελίδα που βρισκόταν (ή τον πηγαίνω σε κάποια σελίδα που θα λέει ότι συνδεθήκατε ως τάδε μέσω του Facebook).
2. Εφόσον δεν υπάρχει active3 account με το ίδιο email με αυτό που λαμβάνω από το social media τότε μπορώ:
   1. Να προτρέπω το χρήστη να κάνει πρώτα registration μέσω της κανονικής φόρμας του site χρησιμοποιώντας το ίδιο email και από την επόμενη φορά να του επιτρέπω να κάνει login όπως και στο βήμα 1.
   2. Να δημιουργώ ένα προφίλ εκείνη τη στιγμή με ένα random password και ότι στοιχεία πάρω από το social media (όνομα, email κλπ.) και να στέλνω και ένα email στο χρήστη ότι από εδώ και πέρα μπορεί να κάνει login είτε μέσω του social media, είτε κανονικά με το password που του δώσαμε.
3. Ένας χρήστης μπορεί ήδη να είναι συνδεμένος με κάποιο social media σε άλλο tab του browser και μετά να έρθει στο δικό μας site. Σε αυτή την περίπτωση δεν θα πατήσει ποτέ το κουμπί για σύνδεση και τα connection api θα τον θεωρούν συνδεμένο, να προχωρούμε σε αυτόματη σύνδεση του και στο active3 σε αυτή την περίπτωση με το που θα φορτώνει η σελίδα;

Υπάρχουν περιπτώσεις που κάποια sites μπορεί να μην έχουν ελεύθερο registration, ή να είναι ελεύθερο αλλά να απαιτούν κάποια στοιχεία τα οποία δεν είναι απαραίτητο ότι θα τα πάρουμε από το social media (π.χ. διεύθυνση, τηλέφωνο κλπ). Για να καλύψω αυτές τις περιπτώσεις θα κάνω παραμετρική τη επιλογή συμπεριφοράς του βήματος 2 ώστε να μπορεί να ρυθμιστεί ένα site να δουλεύει και με τους δύο τρόπους.

Με τη εξέλιξη σχετικά με το twitter προφανώς έχω πρόβλημα στο να υλοποιήσω τη διασύνδεση με αυτόν τον τρόπο καθώς δεν μπορώ να πάρω το email του χρήστη και να το κάνω match. Πρέπει ίσως να δούμε τη λύση που περιγράφω στο τέλος.

# Διαδικασία αποσύνδεσης

Ο χρήστης έχει κάνει πετυχημένη σύνδεση στο site μας μέσω κάποιου social media, από εκεί και πέρα θα ισχύει ότι ισχύει για τους χρήστες του active3 που σημαίνει ότι θα κάνει logoff από το site από το κλασσικό κουμπί και όχι μέσω των social media.

Δεν γίνεται να συνδέσουμε τυχών αποσύνδεση ενός χρήστη από το social με αποσύνδεση και από το site γιατί αυτός μπορεί απλά να θέλει να κλείσει το Facebook αλλά όχι και να αποσυνδεθεί από εμάς. Επίσης μπορεί να είναι συνδεμένος και με Facebook και με το Gmail και απλά να κλείσει το ένα από τα δύο.

Υπάρχει νόημα να συνεχίσουμε να του εμφανίζουμε κουμπιά για «αποσύνδεση» από τα social media αφού έχει συνδεθεί από τη στιγμή που αυτά τα κουμπιά θα το αποσυνδέουν μόνο από το social media και όχι από το δικό μας site.

# Γενικότερες παρατηρήσεις / προβλήματα

## Account hijacking

Τα email που λαμβάνουμε από τα social media είναι συνήθως verified. Αντίθετα στο active3 μπορώ να δηλώσω ότι email θέλω. Θα μπορούσε ένας χρήστης να δημιουργήσει ένα account στο active3 με το email κάποιου άλλου και αν τυχών αυτός ο άλλος συνδεθεί μέσω social media τότε ο πρώτος θα έχει το original password του active3 και θα μπαίνουν και οι δύο στο ίδιο account.

## Multiple emails / No email (twitter)

Ένας χρήστης μπορεί να έχει δώσει διαφορετικό email (ή να έχει περισσότερα από ένα email π.χ. work, home, personal) σε κάθε social media. Προφανώς το να βασίσουμε την ύπαρξη του χρήστη στο κατά πόσο υπάρχει το email που έδωσε στο social media στον πίνακα των Users μπορεί να δημιουργήσει προβλήματα καθότι ο ίδιος χρήστης ενδέχεται να αποκτήσει πολλαπλά accounts λόγω των διαφορετικών email που έχει δώσει σε κάθε social media.

Η πιο σωστή λύση θα ήταν να υπήρχε η δυνατότητα από το προφίλ του κάθε χρήστη να μπορεί να συνδέσει το Facebook, google+, twitter account του και η συσχέτιση να βασιστεί σε κάποιο ID. Με αυτό τον τρόπο θα μπορούσε να λειτουργεί η διασύνδεση με όλα τα social media ανεξάρτητα από το email που έχει δώσει στο καθένα (και να παρακάμψουμε το γεγονός ότι το twitter δεν μας δίνει email). Αυτό βέβαια συνεπάγεται ότι ο χρήστης θα πρέπει **την πρώτη φορά** να κάνει κανονικά registration μέσω της active3 φόρμας και μετά από τη διαχείριση του προφίλ του να προχωράει σε διασύνδεση με όποιο social media θέλει. Φυσικά θα πρέπει να αναπτυχθεί και η δυνατότητα forget me.

Πρακτικά σημαίνει ότι το single click sign in θα δουλεύει μόνο εφόσον έχει γίνει registration και επιπλέον σύνδεση του προφίλ με τα social media (Όχι τόσο straightforward). Δεν θα επιτρέπεται η δημιουργία νέου χρήστη απευθείας από τα social media.